Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

GDK Schweizerische Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren
CDS Conférence suisse des directrices et directeurs cantonaux de la santé
CDS Conferenza svizzera delle direttrici e dei direttori cantonali della sanità

eHealth Suisse

Standards und Architektur Empfehlungen IV

Kommunikation zwischen Gemeinschaften / Zugangsportal

Verabschiedet vom Steuerungsausschuss

Bern, 17. Januar 2013

ehealthsuisse
Koordinationsorgan Bund-Kantone
Organe de coordination Confédération-cantons
Organi di coordinamento Confederazione-Cantoni

Impressum

Projektorganisation
Steuerungsausschuss: Alain Berset (Bundesrat, Vorsteher EDI); Pascal Strupler (Direktor BAG); Stefan Spycher (Vizedirektor BAG); Andreas Faller (Vizedirektor BAG bis Dezember 2012); Carlo Conti (Regierungsrat, Vorsteher GD BS); Guido Graf (Regierungsrat, Vorsteher GD LU); Heidi Hanselmann (Regierungsrätin, Vorsteherin GD SG); Pierre-François Unger (Regierungsrat, Vorsteher GD GE).
Projektleitungsgremium: Adrian Schmid („eHealth Suisse“, Vorsitz); Christian Affolter (santésuisse); Lotte Arnold (SPO); Hansjörg Looser (GD SG); Daniel Notter, (pharmaSuisse); Caroline Piana, (H+); Georg Schielke, (GDK); Michael Stettler (BAG bis März 2012); Adrian Jaggi (BAG bis Dezember 2012); Walter Stüdeli (IG eHealth); Salome von Greyerz (BAG); Judith Wagner (FMH).

Geschäftsstelle „eHealth Suisse“: Adrian Schmid (Leitung), Catherine Bugmann, Isabelle Hofmänner, Sang-Il Kim, Stefan Wyss.

Fachliche Beratung: Christian Lovis (Hôpitaux Universitaires de Genève HUG, Präsident SGMI)

Weitere Informationen und Bezugsquelle:
www.e-health-suisse.ch

Zweck und Positionierung dieses Dokuments

Der Steuerungsausschuss von Bund und Kantonen zur Umsetzung der „Strategie eHealth Schweiz" hat am 20. August 2009, am 20. Oktober 2010 und am 27. Oktober 2011 in diversen Themen Empfehlungen verabschiedet. Zudem wurde am 27. Januar 2011 das Evaluationskonzept Modellversuche verabschiedet. Das vorliegende Dokument enthält Vorschläge für weitere Empfehlungen im Bereich von „Standards und Architektur". Als Vorbereitung dienten zwei Inputarbeiten des Firmenkonsortiums Post/ELCA (Kommunikation zwischen Gemeinschaften) und der Firma Swisscom in Zusammenarbeit mit medshare GmbH und Health On the Net Foundation HON (Zugangsportal). Die Empfehlungsdokumente und die Vorbereitungsarbeiten sind zugänglich unter www.e-health-suisse.ch.

Im Interesse einer besseren Lesbarkeit wurde auf die konsequente gemeinsame Nennung der männlichen und weiblichen Form verzichtet. Wo nicht anders angegeben, sind immer beide Geschlechter gemeint.

1 Ausgangslage ... 3
1.1 Einleitung ... 3
1.2 Abgrenzung ... 4
1.3 Begriffe ... 5
2 Zentrale Komponenten und Dienste ... 8
3 Kommunikation zwischen Gemeinschaften ... 11
3.1 Allgemeine Grundsätze ... 11
3.2 Berechtigungskonzept ... 12
3.3 Identifikation und Authentisierung ... 14
4 Audit und Notifikation ... 15
5 Zugangsportal ... 18
6 Schlussbemerkungen ... 22
Anhang 1: Relevante Architekturgrundlagen ... 24
Anhang 2: Technische Umsetzungshinweise ... 26
Anhang 3: Attribute CPI-S (Verzeichnisdienst der Gemeinschaften und externen Zugangsportale) ... 30

1 Ausgangslage

1.1 Einleitung

Bisherige Empfehlungen als Basis

Grundlage dieses Dokumentes sind die bisherigen Empfehlungen und Berichte von „eHealth Suisse“, siehe:

http://www.e-health-suisse.ch/umsetzung/00146/00148/index.html?lang=de

Positionierung des vorliegenden Dokumentes

Das vorliegende Dokument beschreibt auf fachlicher Ebene, wie die Kommunikation zwischen Gemeinschaften sichergestellt werden kann, welche zentralen Komponenten dafür notwendig sind und wie die Architekturkomponente „Zugangsportal“ ausgestaltet ist. Zum Teil definiert das Dokument neue Aufgaben, deren Zuständigkeit noch offen ist. Diese Zuständigkeit sowie die der Verbindlichkeit bei der Anwendung sind politische Entscheide, die im Rahmen der Rechtsetzungsprojekte geklärt werden müssen. Denkbar sind rechtliche Grundlagen auf Bundes- oder Kantonsebene – oder vertragliche Vereinbarungen zwischen den Akteuren.

Bedeutung der Kommunikation

Die in der Folge empfohlenen Konzepte beziehen sich in der „Architektur eHealth Schweiz“ auf die Kommunikation zwischen Gemeinschaften (unter Einbezug der schweizweit koordinierten Komponenten) sowie auf die Architekturkomponente „Zugangsportal Bevölkerung/Patienten“ (siehe Abbildung 1). Damit werden weitere wichtige Bausteine der Gesamtarchitektur „eHealth“ Schweiz beschrieben, die für den föderalen dezentralen Lösungsansatz notwendig sind.

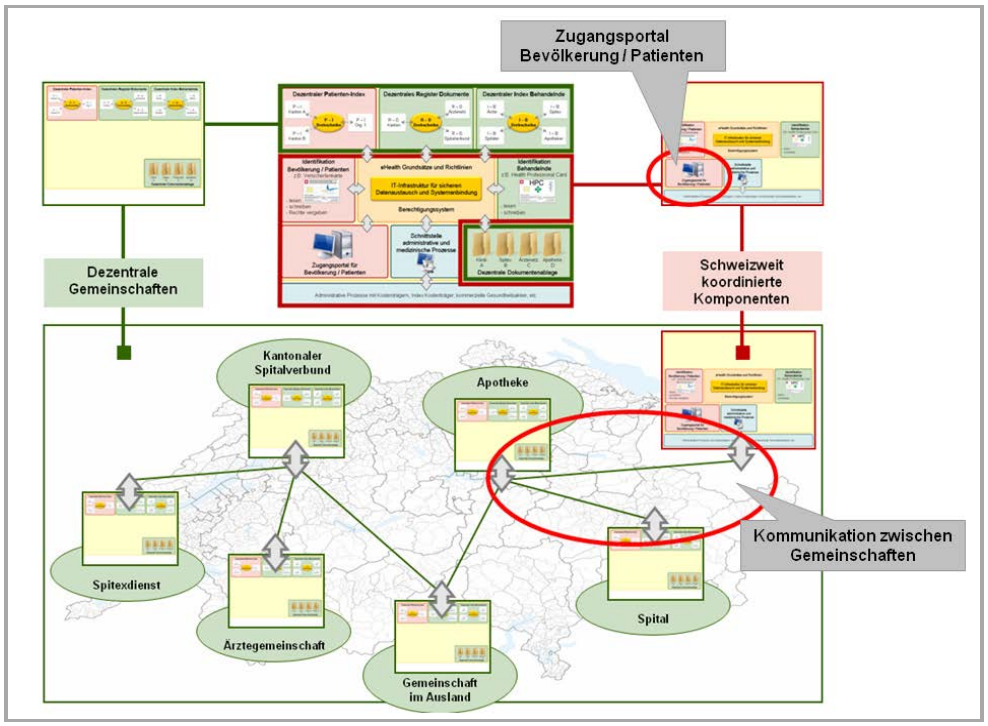


Abbildung 1: Positionierung in der "Architektur eHealth Schweiz"

In den Empfehlungen I bis III lag das Hauptaugenmerk auf den dezentralen Komponenten in den Gemeinschaften und den Basiskonzepten für die Schweiz weite Berechtigungssteuerung. Nun wird definiert, mit welchen Komponenten und Abläufen die Kommunikation zwischen Gemeinschaften gestaltet werden soll. Der Anhang 1 „Relevante Architekturgrundlagen" zeigt eine Übersicht der dafür relevanten früheren Empfehlungen.

Ergänzung zu Empfehlungen I bis III

1.2 Abgrenzung

Die Entwicklung von „eHealth“ ist ein evolutionärer Prozess, der verschiedene Reifegrade durchläuft. Abbildung 2 zeigt schematisch ein mehrstufiges Maturitätsmodell, das einen Transitionsprozess von heute schon existierenden Lösungen hin zu zukünftigen aufzeigt.

Reifegradmodell

- Reifegrad 1: Gerichtete elektronische Kommunikation (zum Beispiel Punkt zu Punkt, eMail mit Dokumentenanhängen, etc.). Das Informationssystem der Behandelnden[1] ist der „Primärspeicher" der Dokumente;
- Reifegrad 2: Dokumentenzentriertes System für eine ungerichtete Kommunikation. Zeitlich unabhängiges Bereitstellen und Abfragen von mehr oder weniger strukturierten Dokumenten, die dezentral als Kopie in einem „Sekundärspeicher“ abgelegt werden (Elektronisches Patientendossier EPD);
- Reifegrad 3: Datenzentriertes System mit multidimensionaler Verfügbarkeit von strukturierten Daten. Direkte Eingabe von medizinischen Informationen in ein EPD. Die Grenze zwischen „Primärspeicher" und „Sekundärspeicher" verschwimmt zusehends. Die Behandelnden werden durch „Decision Support Systeme“ unterstützt.

Die bisherigen Empfehlungen I-III und die vorliegenden Empfehlungen IV beziehen sich auf den Reifegrad 2 im Sinne der „Strategie eHealth Schweiz" mit dem Ziel ein schweizweites elektronisches Patientendossier zu etablieren. Zwischen den Reifegraden 2 und 3 bestehen folgende wesentliche Unterschiede:

- Beim Reifegrad 2 ist nur das zeitlich versetzte Bearbeiten von Dokumenten möglich (asynchron). Der Reifegrad 3 erlaubt die gleichzeitige Bearbeitung von Dokumenten durch mehrere Benutzer (synchron);
- Beim Reifegrad 2 werden abgeschlossene Informationseinheiten in einem EPD zur Verfügung gestellt. Beim Reifegrad 3 können auch „frei verfügbare" Daten bearbeitet werden, die multidimensional verknüpft werden können.

Technisch und funktional folgen die Reifegrade 1 bis 3 nacheinander. Beim Informationsinhalt, der Datennutzung und den regulatorischen Rahmenbedingungen können sie nebeneinander existieren. Damit wird ermöglicht, dass eine angemessene, bedürfnisorientierte Entwicklung geschehen kann, die den gesellschaftlichen und wirtschaftlichen Herausforderungen gerecht wird. Ziel sollte dabei immer sein, dass die Interoperabilität der Daten zwi-

[1] Im Kontext des Gesetzentwurfs für das elektronische Patientendossier wird anstatt vom "Behandelnden" von der "Gesundheitsfachperson" geredet.

schen den verschiedenen Reifegraden gewährleistet ist. Die Empfehlungen I bis IV von „eHealth Suisse“ beschränken sich auf den Reifegrad 2. Wann der Reifegrad 3 eingeläutet wird, kann derzeit nicht abgeschätzt werden. Innerhalb von Institutionen und Organisationen ist sie heute schon vereinzelt anzutreffen, aber noch nicht über Organisationsgrenzen hinweg.

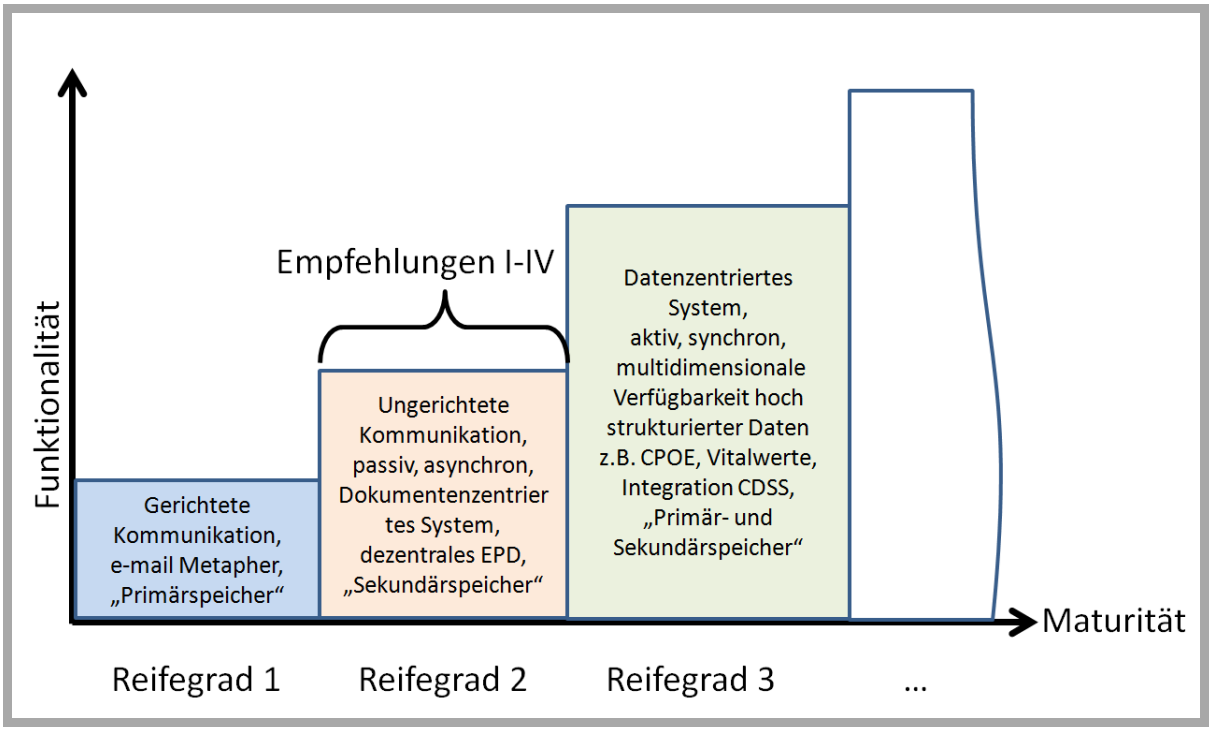


Abbildung 2: Reifegrad-Modell „eHealth“-Evolution

1.3 Begriffe

Eine Gemeinschaft ist eine organisatorische Einheit von Behandelnden, die Gemeinschaft

1. an der Patientenbehandlung beteiligt ist und
2. patientenbezogene Informationen erstellt und verwendet und
3. patientenbezogene Informationen mit anderen Gemeinschaften austauscht.

Die Zusammenarbeit innerhalb einer Gemeinschaft ist vertraglich zu regeln und Bedarf einer Rechtsform. Einzelne Behandelnde können mehreren Gemeinschaften angehören. Die Definition enthält keine Vorgaben bezüglich der Grösse, der geografischen Abgrenzung oder der organisatorischen Struktur einer Gemeinschaft. Folgende Auflistung gibt Hinweise auf mögliche Ausprägungen von Gemeinschaften:

- Zusammenschluss von Behandelnden verschiedener Kategorien (z.B. Arztpraxen, Physiotherapeuten, Spitäler) in einer Region zu einem Versorgungsnetzwerk, auch über Kantonsgrenzen hinweg;
- Spitalverbünde, die eng miteinander kooperieren und Patienten austauschen, zum Beispiel ein Zentrumsspital mit mehreren kleineren Spitälern;

- Ärztenetzwerke, die entweder lokal oder regional organisiert sind und deren Mitglieder eng kooperieren, z.B. ein onkologisches Netzwerk;
- Zusammenschluss von Organisationen einer Behandelndengruppe aus synergistischen Gründen, z.B. mehrere Labore, die medizinische Daten anderen Gemeinschaften zur Verfügung stellen wollen oder viele Apotheken, die ihren Kunden zusätzliche Services anbieten wollen.

Die Gemeinschaften, die am Gesamtsystem „eHealth Schweiz“ teilnehmen wollen, müssen sich in Bezug auf Technik, Prozesse und Organisation zertifizieren lassen.

In der Folge wird unter dem Begriff "Gemeinschaft" und "Zugangsportal" im vorliegenden Dokument immer eine Zertifizierung vorausgesetzt.

Stammgemeinschaft

Jede Stammgemeinschaft muss Funktionen für die Verwaltung der Einverständniserklärungen und Berechtigungen anbieten. Gemeinschaften, welche diese Funktionen nicht anbieten, können von den Patienten nicht als Stammgemeinschaft gewählt werden. Damit die Patienten die Zugriffsberechtigungen für ihr Dossier regeln können, muss jede Stammgemeinschaft ein internes Zugangsportal anbieten. Beim Wechsel der Stammgemeinschaft müssen die Berechtigungen in die neue Stammgemeinschaft mitgenommen werden können. Die Stammgemeinschaft muss sicherstellen, dass dies möglich ist (Export in neue Stammgemeinschaft, Import von Daten aus einer anderen Stammgemeinschaft). Zu jeder Patientenidentität kann zu einem Zeitpunkt immer nur eine Stammgemeinschaft existieren. Auch Stammgemeinschaften müssen sich wie Gemeinschaften zertifizieren lassen.

Zugangsportal

Der Patient soll jederzeit selber auf die eigenen Daten zugreifen können. Damit ist ein wesentlicher Anspruch auf Datentransparenz und Selbstbestimmung der Patienten erfüllt. Dieses Zugriffsrecht wird über zertifizierte Zugangsportale (interne oder externe) sichergestellt. Zusätzlich soll das interne Zugangsportal den Benutzern die Verwaltung der individuellen Zugriffsrechte ermöglichen.

Ein „internes“ Zugangsportal kann ein integraler Bestandteil einer Gemeinschaft sein. Unabhängige „externe“ Zugangsportale ausserhalb einer Gemeinschaft sind jedoch auch möglich, diese bieten nur lesende Zugriffe und keine Möglichkeit Daten hochzuladen oder Berechtigungen zu verändern.

Die Patienten sollen über das interne Zugangsportal auch eigene persönlich erhobene Daten wie Schmerztagebuch, Blutzuckerwerte oder Blutdruckwerte den Behandelnden zugänglich machen können.

Ausser den Patienten sollen auch berechtigte Behandelnde die internen Zugangsportale nutzen können für die Dateneinsicht oder die Dateneingabe.

Folgende Tabelle zeigt die beiden Typen von Zugangsportalen und die wichtigsten Funktionalitäten für die potentiellen Benutzer. Alle Benutzer müssen entweder in der Gemeinschaft oder am externen Zugangsportal registriert sein, um ein Systemteilnehmer zu sein, auch die Behandelnden, die keiner Gemeinschaft angehören und das externe Zugangsportal nutzen wollen.

internes Zugangsportal in (Stamm-)Gemeinschaft		externes Zugangsportal ohne Gemeinschaft, nur lesende Zugriffe	
Patient	Behandelnde ohne IT-Integration[2]	Patient	Behandelnde ohne IT-Integration
-Verwaltung Berechtigung -Einsicht Daten -Speichern Daten	-Einsicht Daten -Speichern Daten	-Einsicht Daten	-Eventuell Einsicht Daten

Zugangspunkt

Ein Zugangspunkt ist die *logische* Sicht von aussen auf eine Gemeinschaft. Eine Gemeinschaft kommuniziert ausschliesslich über den Zugangspunkt mit anderen Gemeinschaften.

Gateways

Ein Zugangspunkt muss mehrere Funktionen erfüllen. Diese werden *technisch* als Gateways implementiert. Ein Gateway erfüllt eine bestimmte Aufgabe, indem er einen Dienst anbietet oder nutzt. Der Zugangspunkt einer Gemeinschaft umfasst somit mehrere Gateways, zum Beispiel anfragender (initiating) Gateway und antwortender (responding) Gateway. Die einzelnen Gateways einer Gemeinschaft sind zu zertifizieren.

Der Anhang 2 beschreibt für jedes der vier folgenden Kapitel 2 bis 5 wichtige Themen der technischen Umsetzung.

[2] Behandelnde, die entweder keine elektronischen Krankenakten benutzen oder deren IT-Systeme noch nicht direkt mit der EPD-Infrastruktur integriert sind, z.B. ein Arztpraxissoftwaresystem, das kein IHE Profil unterstützt oder ein Spital-IT-System das medizinische Dokumente nicht selber registrieren kann.

2 Zentrale Komponenten und Dienste

Sicherer Raum dank Zertifizierung

Die elektronische Kommunikation innerhalb der „Architektur eHealth Schweiz“ hat folgende Merkmale:

- Kommunikationsraum im Internet, d.h. alle digitalen Transaktionen werden über das weltweite Internet übermittelt;
- Starke Authentifizierung der Benutzer;
- Sicherung der Kommunikationswege und der transportierten Daten durch Verschlüsselung;
- Punkt-zu-Punkt Kommunikation zwischen den Zugangspunkten.

Diese Merkmale ergeben einen gesicherten Kommunikationsraum im Internet (EPD-Vertrauensraum). Daran teilnehmen können Gemeinschaften und Zugangsportale über Zugangspunkte, die ein oder mehrere technische Gateways beinhalten können (siehe Abbildung 3). Die notwendigen zentralen Komponenten sind systemkritisch und müssen daher hohen Qualitätsrichtlinien entsprechen.

Empfehlung 1

Vertrauensraum durch Zertifizierung

Die Zugangspunkte der Gemeinschaften und der Zugangsportale sowie die zentralen Komponenten bilden den EPD-Vertrauensraum. Alle Zugangspunkte sind zertifiziert.

Empfehlung 2

Aussensichten aller Gateways identisch

Aus der Aussensicht als Zugangspunkt zum EPD-Vertrauensraum funktionieren alle Gateways identisch, dies gilt insbesondere auch für die externen Zugangsportale ausserhalb von Gemeinschaften

„Zentrale" Services

Für eine reibungslose Kommunikation zwischen Gemeinschaften werden „zentrale" Verzeichnisservices benötigt. Abbildung 3 zeigt diese schematisch:

- Verzeichnis der Gemeinschaften und externe Zugangsportale: Community / Portal Index (CPI-S);
- Verzeichnis der Behandelnden:
  Healthcare Professional Index-Service (HPI-S);
- Verzeichnis der Gesundheitsorganisationen:
  Healthcare Organisation Index-Service (HOI-S);
- Verzeichnis der Rollen:
  Rollen Index-Service (RI-S);
- Verzeichnis der Dokumenten-Metadaten:
  Metadaten Index-Service (MDI-S).

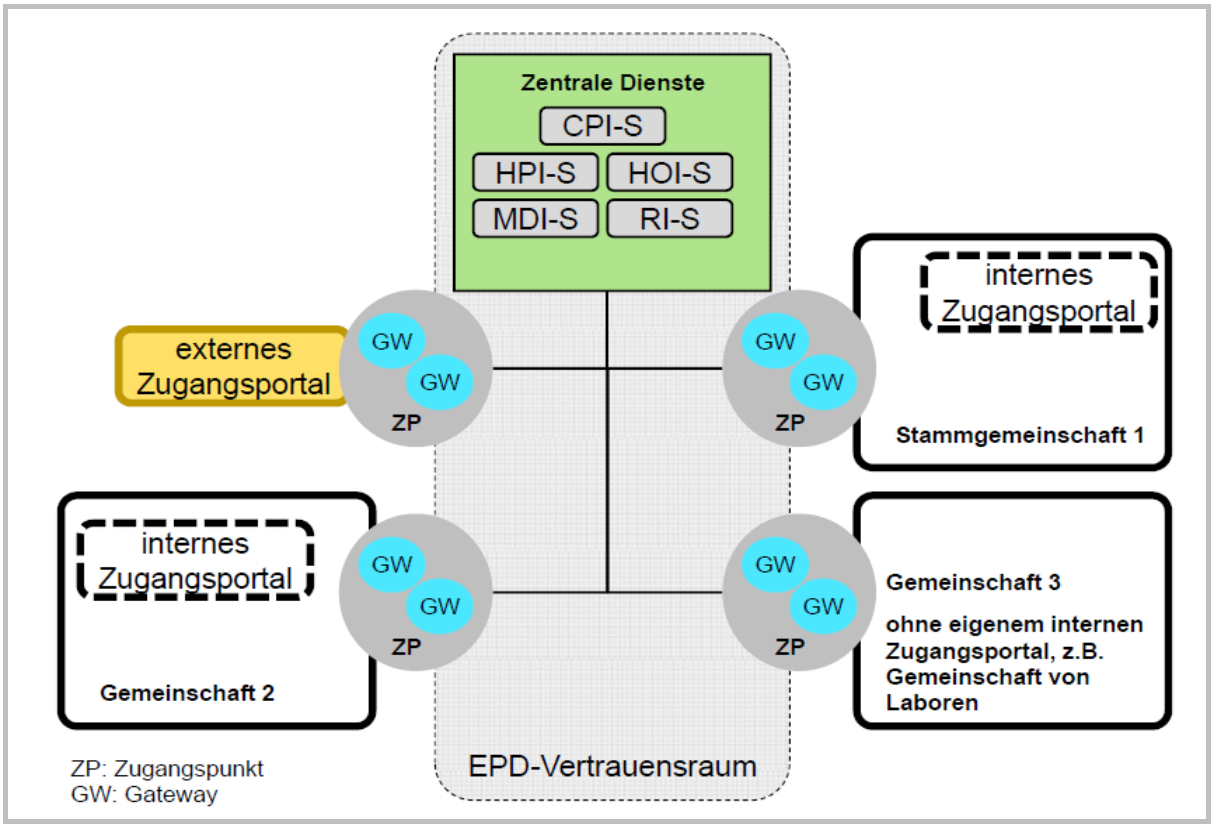


Abbildung 3: EPD-Vertrauensraum und zentrale Komponenten/Services

Im Vergleich zu den Empfehlungen II (siehe Seite 12, Empf.3) wird auch externen Zugangsportalen der lesende Informationsaustausch gewährt. Desweiteren wird die technische Ausgestaltung mit geforderten Attributen definiert. Die notwendigen Angaben sind im Anhang 3 „Attribute CPI-S" aufgeführt.

Jede Gemeinschaft und jedes externe Zugangsportal ist über den zentralen Verzeichnisservice abrufbar. Es führt nur gültig zertifizierte Gemeinschaften und externe Zugangsportale. Die Eintragung im Verzeichnis und die Pflege der Einträge werden zentral vorgenommen.	Empfehlung 3 Zentraler Verzeichnis der Gemeinschaften und externe Zugangsportale

Für die Umsetzung der Zugriffssteuerung auf Daten eines Patienten müssen eindeutig identifizierte Behandelnde einer oder mehreren zugelassenen Rollen zugeordnet werden können. Für die eindeutige Identifikation mit weiteren wichtigen Angaben wie Berufsgruppe und Qualifikation ist ein schweizweiter Health Professional Index Service (HPI-Service) notwendig mit folgenden Angaben:

- GS1 GLN als eindeutiger Identifikator;
- Personenstammdaten;
- Beruf/Qualifikation;
- Fachrichtung (sofern vorhanden);
- Berufsausübungsbewilligung mit Zeitangaben und Angabe der ausgebenden Stelle (sofern vorhanden).

Jeder Behandelnde, der am EPD-Vertrauensraum teilnimmt, ist über den HPI-Service auffindbar und eindeutig identifiziert. Die einzelnen Register liefern dem HPI-Service entsprechende Informationen und garantieren für die Zuverlässigkeit der Daten. Die Verwaltung dieses Services ist schweizweit koordiniert.	Empfehlung 4 Zentraler Verzeichnisdienst der Behandelnden
Ergänzend zu den personenspezifischen Angaben eines Behandelnden ist ein Verzeichnis aller Einrichtungen des Gesundheitswesens notwendig (Spital, Abteilung eines Spitals, Spitex-Organisation, Arztpraxis, etc.), die in einem Health Organisation Index-Service (HOI-Service) abgefragt werden können. Dieses Verzeichnis soll ausser beschreibenden Informationen auch eindeutige GLNs führen (siehe Empfehlungen II, Metadatum 2.5: Institutionen-ID aus GS1 GLN (GS1 Global Location Number). Im Berechtigungssystem kann die Angabe der Organisation in Kombination mit den Personenangaben benutzt werden - zum Beispiel für Zugriffsberechtigung für Mitglieder einer Arztpraxis.	
Die klare Trennung zwischen den Personen und den Einrichtungen im HPI-Service und HOI-Service ist wichtig. Nur so kann aufbauend auf beiden Verzeichnissen die Zugehörigkeit der Personen zu verschiedenen Institutionen abgebildet und die referenzielle Integrität sichergestellt werden (z.B. Arzt XY arbeitet in Arztpraxis A und Spital B).	Zusammenspiel HPI-S und HOI-S
Ein Health Organisation Index (HOI-Service) mit GS1 GLN Einträgen ist als eigener zentraler Service verfügbar. Die Verwaltung dieses Verzeichnisses wird schweizweit koordiniert.	Empfehlung 5 Zentraler Verzeichnisdienst der Gesundheitsorganisationen
Für die Umsetzung des Berechtigungssystems ist ein abrufbares Verzeichnis der zugelassenen Rollen notwendig (Rollenverzeichnis-Service). Der Patient hat jederzeit die Möglichkeit Rollen-IDs den Identitäten von Behandelnden zuzuordnen und damit den Zugriff zu steuern.	
Ein Rollenverzeichnis-Dienst ist als eigener zentraler Service verfügbar. Die Verwaltung dieses Verzeichnisses wird schweizweit koordiniert.	Empfehlung 6 Zentraler Rollenverzeichnis - Dienst
Beim Informationsaustausch zwischen Gemeinschaften, ist die Nutzung von einheitlichen IHE XCA-Metadaten notwendig. Nur so kann eine technische und semantische Interoperabilität gewährleistet werden. Einige Metadatenattribute sind für die Berechtigungssteuerung relevant. Andere sind beschreibend und nutzbar für Filterung und Sortierung in der Darstellung der Daten.	
Ein Metadatenverzeichnis-Dienst steht als eigener zentraler Service zur Verfügung. Die Verwaltung dieses Verzeichnisses wird schweizweit koordiniert.	Empfehlung 7 Zentraler Metadatenverzeichnis - Dienst

3 Kommunikation zwischen Gemeinschaften

3.1 Allgemeine Grundsätze

Wie in Abbildung 3 schematisch dargestellt wird die Kommunikation zwischen den Gemeinschaften nur über die logischen Zugangspunkte einer Gemeinschaft bzw. die technischen Gateways ermöglicht. Dem Grundprinzip folgend, dass ein im System hinterlegtes Dokument eindeutig und nicht mehr veränderbar sein soll, ist eine schreibende Funktionalität über die Gateways nicht erlaubt. Das gilt auch für die über Gateways angebundenen externen Zugangsportale.

Der gemeinschaftsübergreifende Zugriff über die Gateways ist nur lesend ausgestaltet. Jede Gemeinschaft behält so die Hoheit über alle in der Gemeinschaft erzeugten Dokumente mit allen Rechten und Pflichten und kann auch jederzeit zweifelsfrei den Originalinhalt eines Dokuments nachweisen.	Empfehlung 8 Gemeinschafts-übergreifende Zugriffe: Nur lesend

Die eindeutige Zuordnung zu Personen im Kontext der „Architektur eHealth Schweiz" geschieht mittels elektronischer Identitäten. Dabei besteht grundsätzlich die technische Möglichkeit, dass eine Person mehrere elektronische Patientenidentitäten besitzen kann. Die Fragestellung, ob eine Person mit einer oder mehreren elektronischen Identitäten am System teilnehmen kann, ist im Rahmen der Gesetzgebungsprojekte zu klären.

Personenidentitäten

Das Zivilstandsamt der Heimatgemeinde führt ein Register der Gemeindebürgerinnen und Gemeindebürger und stellt Heimatscheine an Privatpersonen aus. Jede Person, die sich in einer Gemeinde neu niederlässt, muss ihren Heimatschein bei der Einwohnerkontrolle hinterlegen. Ähnlich dem Schriftwechsel mit dem Heimatausweis, kann ein Patient seine Einwilligung und Berechtigungsattribute pro Identität nur an einer Stelle hinterlegen und muss sie bei einem Wechsel mitnehmen.

Analogie zum Heimatausweis

Damit Patienteneinwilligung und Zugriffsrechte eindeutig gefunden werden, darf eine elektronische Patientenidentität jederzeit nur einer Stammgemeinschaft zugeordnet werden.

Jede elektronische Patientenidentität ist jederzeit nur einer Stammgemeinschaft zugeordnet.	Empfehlung 9 Eine Stammgemeinschaft pro Identität

Für einige Szenarien sind Export- und Importfunktionalitäten erforderlich. Dazu gehören zum Beispiel der Wechsel eines Patienten in eine andere Stammgemeinschaft, sein Austritt aus einer (Stamm-)Gemeinschaft oder die Schliessung einer (Stamm-)Gemeinschaft. Dabei kann es um medizinische und administrative Daten, Log-Files oder Rechteattribute gehen. Dies impliziert keine schreibende Gateway-Funktionalität in andere Gemeinschaften und auch keine unnötigen Kopien von Daten. Die Schliessung einer (Stamm-)Gemeinschaft führt zum Ausschluss der in dieser Gemeinschaft gespeicherten Daten im EPD. Die Originaldokumente der Behandelnden verbleiben bei den erstellenden Quellsystemen.

Eine Gemeinschaft ist in der Lage alle zu einem Patienten gehörenden Inhalte zu importieren und zu exportieren. Import und Export erfolgen über die Architekturkomponente „Schnittstelle administrative/medizinische Prozesse“. Diese Fähigkeit ist zertifizierungsrelevant.	Empfehlung 10 Funktionalität für Export und Import

3.2 Berechtigungskonzept

Gemäss den Empfehlungen II und III basiert das Berechtigungssystem der „Architektur eHealth Schweiz" einerseits auf der Rolle des Benutzers und der Metadaten eines Dokumentes und andererseits auf den individuellen Einstellungen der Rechteattribute durch den Patienten. Entscheidend ist am Ende immer die explizite Vergabe einer Zustimmung durch den Patienten für die Einsicht in seine Daten, gemäss einer vom Patienten verwalteten dynamischen Zugriffsliste. Das kann zum Beispiel durch die namentliche Nennung von Behandelnden über den HPI-Service geschehen, denen er eine bestimmte Rolle zuordnet. Ein anderer denkbarer Weg ist die explizite Vergabe/Bestimmung von Vertraulichkeitsstufen der Dokumente durch den Patienten, zum Beispiel die Regel, dass alle Dokumente aus einer Psychiatrischen Abteilung immer die Vertraulichkeitsstufe „stigmatisierend" erhalten. In allen Fällen muss der Patient genügend aufgeklärt sein über die Auswirkungen seiner Handlungen bei der Verwaltung seiner Rechteattribute. Somit soll ausgeschlossen werden, dass implizite Regeln/Automatismen ohne das Wissen des Patienten den Zugriff steuern können. Die in der Empfehlung III genannte Grundeinstellung (siehe Seite 20, Empfehlung 5) muss dem Patienten also genau erläutert werden, ebenso sein Recht diese Voreinstellungen explizit verändern zu können.

Der Patient steuert

Die Berechtigungssteuerung basiert auf dem Prinzip der expliziten Vergabe von Zugriffsrechten durch den Patienten. Dies kann über die Metadaten der Dokumente und die Rollenvergabe an bestimmte Behandelnde geschehen. Entscheidend sind die bewusste Handlung des aufgeklärten Patienten und nicht implizite Systemeigenschaften, die dem Patienten unbekannt sind.	Empfehlung 11 Explizite Rechtevergabe durch Patienten

Bei jeder Zugriffsprüfung müssen die Rechteattribute des Patienten ausgewertet werden. Eindeutigkeit und Aktualität der Rechteattribute können am besten gewährleistet werden, wenn diese nur einmal im System vorkommen und keine Kopien davon existieren. Als Ablageort eignet sich die Stammgemeinschaft, da jeder Patientenidentität genau eine Stammgemeinschaft zugeordnet wird (siehe oben). Somit besitzt jede Stammgemeinschaft eine Rechteattribute-Datenbank (RADB) in der alle Rechteattribute-Sets ihrer Patienten abgelegt sind (siehe Abbildung 4).

Berechtigungsattribute einer elektronischen Patientenidentität werden ausschliesslich in der Stammgemeinschaft gespeichert. Die Verwaltung der Berechtigungen erfolgt ausschliesslich in der Stammgemeinschaft. Bei einem Wechsel einer Stammgemeinschaft bedeutet das ein Überführen des Rechteattribute-Sets eines Patienten von der alten in die neue Stammgemeinschaft.	Empfehlung 12 Rechteattribute und Rechteverwaltung in Stammgemeinschaft

Prüfung der Zugriffsrechte

Für die Zugriffssteuerung muss in der anfragenden Gemeinschaft zuerst die Identitätsprüfung erfolgen (technisch im Initiating Gateway), die folgende Berechtigungsprüfung liegt in der Verantwortung der antwortenden Gemeinschaft (technisch im Responding Gateway). Für die Berechtigungsprüfung muss das Rechteattribute-Set des Patienten aus der Stammgemeinschaft gelesen und ausgewertet werden. Damit existiert wie in Abbildung 4 dargestellt ein verteiltes Management der Personen und Zugriffe.

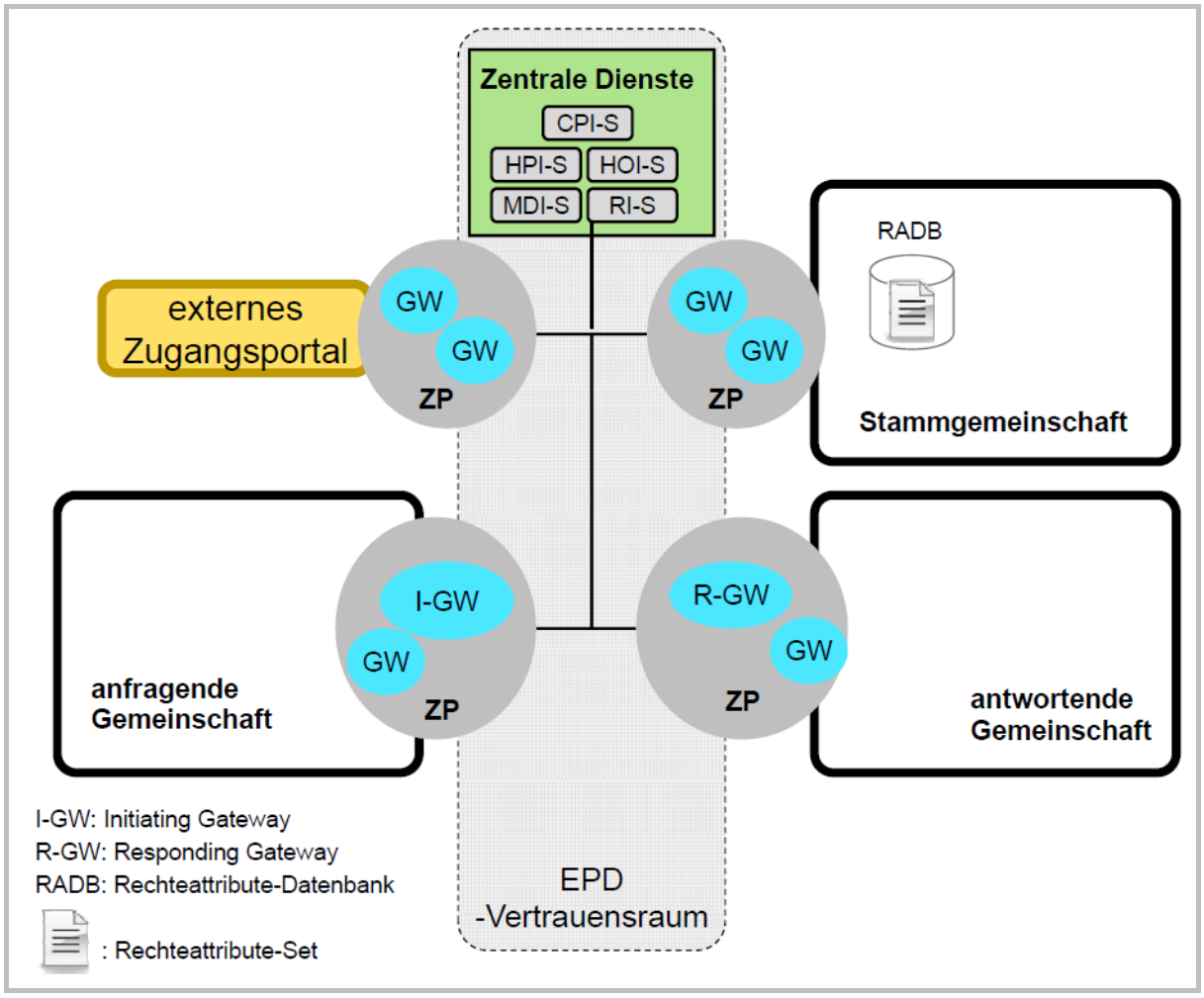


Abbildung 4: Verteiltes Identity und Access Management und Rechteattribute in Stammgemeinschaft

Eine möglichst frühe Berechtigungsprüfung erscheint sinnvoll, weil unnötige nachgelagerte Aktionen vermieden werden können. Zudem vermindert die frühe Durchsetzung von Berechtigungen ein fehlerhaftes Verbreiten schützenswerter Daten. Jedoch können nicht alle Zugriffe bereits im Voraus entschieden werden.

So kann bei Zugriffen auf ein Dokumenten-Register die Berechtigung erst nach dem Zugriff durchgeführt werden, weil jedes Resultat der Suche einzeln geprüft werden muss. Bei Zugriffen auf ein Dokumenten-Repository soll die Prüfung jedoch vor dem Zugriff erfolgen.

Grundsätzlich werden Zugriffe so früh als möglich hinsichtlich der Berechtigungen geprüft. Dabei prüft und entscheidet das antwortende Gateway (responding gateway) der datenhaltenden Gemeinschaft, ob die notwendigen Berechtigungen vorliegen.	Empfehlung 13 Frühe Prüfung der Zugriffsrechte

3.3 Identifikation und Authentisierung

Obwohl das Integrationsprofil IHE:XUA nicht für den spezifischen Einsatz im gemeinschaftsübergreifenden Einsatz entwickelt wurde, lässt es sich durch gezielte Platzierung der beiden Akteure „User Authentication Provider“ und „X-Assertion Provider“ ohne Veränderung einsetzen.	Abfrage von Identitäten zwischen Gemeinschaften
Für die gemeinschaftsübergreifende Vertrauensstellung von Identitäten in Transaktionen wird das IHE:XUA Integrationsprofil eingesetzt.	Empfehlung 14 IHE:XUA-Einsatz auch zwischen Gemeinschaften

4 Audit und Notifikation

Ziel

Das Ziel von Audit (Protokollierung) und Notifikation (Benachrichtigung) ist es, Zugriffe und Änderungen am Patientendossier dem Patienten in nachvollziehbarer Weise aufzuzeigen.

Sowohl Audit wie auch Notifikation dienen dazu, die Sicherheitsanforderungen im Rahmen der Integrität und der Zurechenbarkeit zu erfüllen. Sie unterscheiden sich in folgenden Punkten:

- Audit: Alle Zugriffe auf das EPD werden in einem Ereignisprotokoll gespeichert. Das Erstellen von Einträgen kann nicht unterbunden werden;
- Notifikation: Erlaubt es, den Patienten zu kontaktieren und ihn über Zugriffe auf sein Patientendossier aktiv zu informieren. Notifikationen können durch den Patienten konfiguriert und ausgeschaltet werden. Der Prozess wird durch eine Manipulation am EPD durch einen Behandelnden angestossen.

Bestimmungen zum Datenschutz

Protokolldateien könnten aber auch auf alternativen Wegen betrachtet werden (z.B. durch Administratoren). Deshalb sollen Protokolldateien keine schützenswerten Informationen enthalten, wie zum Beispiel die Inhalte der medizinischen Dokumente. Minimale Informationen wie gewisse Metadaten der Dokumente sind für die Arbeit der Administratoren jedoch notwendig. Da in den Metadaten vertrauliche Informationen enthalten sein können, müssen definierte Prozesse und Regeln für die Administratoren gelten.

Generell speichern Protokolldateien nur die Zugriffsereignisse mit entsprechenden Suchparametern. Die Suchergebnisse selbst, zum Beispiel Inhalte von Dokumenten, dürfen nicht gespeichert werden.	Empfehlung 15 Nur Zugriffsereignisse und keine Ergebnisse

Es gibt keine gemeinschaftsübergreifende Administrator-Rollen. Ein Administrator ist für ein System beziehungsweise für eine Gemeinschaft zuständig. Sämtliche Zugriffe, auch von Administratoren, werden protokolliert.	Empfehlung 16 Administratoren in Gemeinschaften

Standardisierte Auditeinträge

Für eine patientenorientierte Gestaltung der technischen Auditeinträge müssen diese einheitlich aufbereitet und schweizweit standardisiert werden. Die Einträge müssen für die Patienten nachvollziehbar sein und eine sinnvolle Granularität aufweisen. Minimal beantworten sie folgende Fragen:

- Wann erfolgte das Ereignis (Zeitstempel)?;
- Welche Gemeinschaft/System ist betroffen?;
- Wer hat die Aktion ausgelöst (Identifikation der Person/Rolle/Gemeinschaft)?;
- Welcher Patient ist betroffen?;
- Auf welches Informationsobjekt erfolgte der Zugriff?;
- Welche Aktion wurde ausgeführt? Lesen oder Schreiben?;
- Bei Änderung von Einwilligung und Rechten: welche Rechte haben geändert und wie? Alle einzelnen Veränderungen der Rechtematrix werden protokolliert;
- War die Aktion erfolgreich? Auch erfolglose Zugriffsversuche werden protokolliert.

Darüber hinaus können weitere zwingend zu protokollierende Ereignisse festgelegt werden wie zum Beispiel der technische Ausfall eines Systems.

Die Vorgaben und Regelungen für Systemadministratoren und Aufbewahrungsdauer von System-Protokolldaten werden rechtlich festgelegt.

Patientenzentrierte Einsicht in Auditeinträge

Patienten haben jederzeit das Recht, die sie betreffenden Auditeinträge aus allen Gemeinschaften mit sämtlichen Zugriffen auf das eigene Patientendossier einzusehen. Eine entsprechende Umsetzung kann in verschiedenen Varianten erfolgen.

1. Jede Gemeinschaft sendet aktiv die lokalen Ereignisse über Notifikation an die Stammgemeinschaft des Patienten (pull on notification).
2. Jede Gemeinschaft wartet passiv, bis sie eine Anfrage zum Auslesen erhält. Zum Anzeigen aller Zugriffe werden aus einem Zugangsportal (intern oder extern) Anfragen an die Gemeinschaften versendet und die lokalen Auditeinträge ad hoc ausgelesen (pull on request).
3. Lokale Ereignisse werden periodisch pro Gemeinschaft ausgewertet und als eigenständiges Protokoll-Dokument ins Patientendossier eingepflegt.

Für die Varianten 1 und 2 existieren derzeit keine geeigneten IHE-Profile und müssten neu definiert werden. Variante 2 kann nach der Aufbewahrungsdauer von einem Jahr keine Einsicht zu älteren Zugriffen mehr sicherstellen.

Auditeinträge als „Dokument“

In der empfohlenen Variante 3 analysieren die Gemeinschaften periodisch gemäss Wahl des Patienten (z.B. täglich) die Auditeinträge. Dieses Dokument wird über Metadaten in der höchsten Vertraulichkeitsstufe (geheim) und einem eigenen Dokumententyp (audit extract) wie andere medizinische Dokumente im Dokumentenregister der Gemeinschaft eingetragen. Alle zu einer bestimmten Patientenidentifikation zusammengehörenden Extrakte von Systemereignissen werden automatisch als strukturiertes Dokument (CDA Body Level 3) generiert. Zudem muss es lesergerecht als eigenständiges Dokument dargestellt werden. Damit können aus Sicht eines Patienten die Auditeinträge aus allen Gemeinschaften mit den ordentlichen Abfragemechanismen jederzeit ausgelesen werden.

Gemeinschaften werten periodisch die Auditeinträge aus und generieren automatisch patientenzentrierte Protokoll-Dokumente im Format CDA Body Level 3. Sie werden wie ein medizinisches Dokument behandelt.	Empfehlung 17 Patientenzentrierte Protokoll-Dokumente pro Gemeinschaft

Der Patient kann das Intervall für die Zusammenfassung der Ereignisse wählen (täglich, wöchentlich, monatlich). Ebenso kann er die voreingestellte Vertraulichkeitsstufe ändern und damit auch Behandelnden Einsicht gewähren. Auditeinträge (z.B. Änderung von Rechten, Austrittserklärung) sollen aus Gründen der Nachvollziehbarkeit erhalten bleiben. So könnten diese für forensische oder juristische Belange auch viele Jahre nach dem Ereignis relevant sein. Der Patient kann aber jederzeit verlangen, dass Dokumente des entsprechenden Dokumententyps nicht mehr angezeigt werden.

Die Aufbewahrungsfrist der patientenzentrierten Dokumente (inkl. Protokoll-Dokumente) und der Auditeinträge werden rechtlich festgelegt.

5 Zugangsportal

Zentrales Element der „Architektur eHealth Schweiz“

Das Zugangsportal ist ein wesentliches Element der „Architektur eHealth Schweiz“ (siehe Definition Seite 6f). Es ermöglicht Patientinnen und Patienten einen Orts- und zeit-unabhängigen, sicheren und zurück verfolgbaren Zugang auf die Daten des eigenen Elektronischen Patientendossiers (EPD) ohne die Hilfe von Dritten. Darüber hinaus kann der Patient den Datenzugriff mittels individueller Einwilligungen und Rechtevergabe regeln. Es ist die einzige Architektur-Komponente, die sich direkt an den Bürger, beziehungsweise an den Patienten wendet. Durch seine hohe Visibilität wird es massgeblich zur Akzeptanz und zum Erfolg des Systems „eHealth“ Schweiz beitragen können.

externe Portale verhalten sich wie Gemeinschaften

Zugangsportale ermöglichen Interaktionen zwischen den Benutzern, wie Patienten und Behandelnde, mit dem EPD-Vertrauensraum. Sie sind am Zugangspunkt technisch identisch mit den Gemeinschaften, d.h. in der zu zertifizierenden Aussensicht funktionieren alle Gateways identisch. Für Zugangsportale gibt es keinen Sonderfall.

Empfehlung 18

Zwei Varianten von Zugangsportalen

Zugangsportale gibt es in zwei Varianten:

- interne Zugangsportale können *innerhalb* einer Gemeinschaft platziert werden und über den Zugangspunkt ihrer Gemeinschaft kommunizieren;
- externe Zugangsportale können *unabhängig* von Gemeinschaften direkt über eigene Zugangspunkte mit anderen Zugangspunkten von Gemeinschaften kommunizieren.

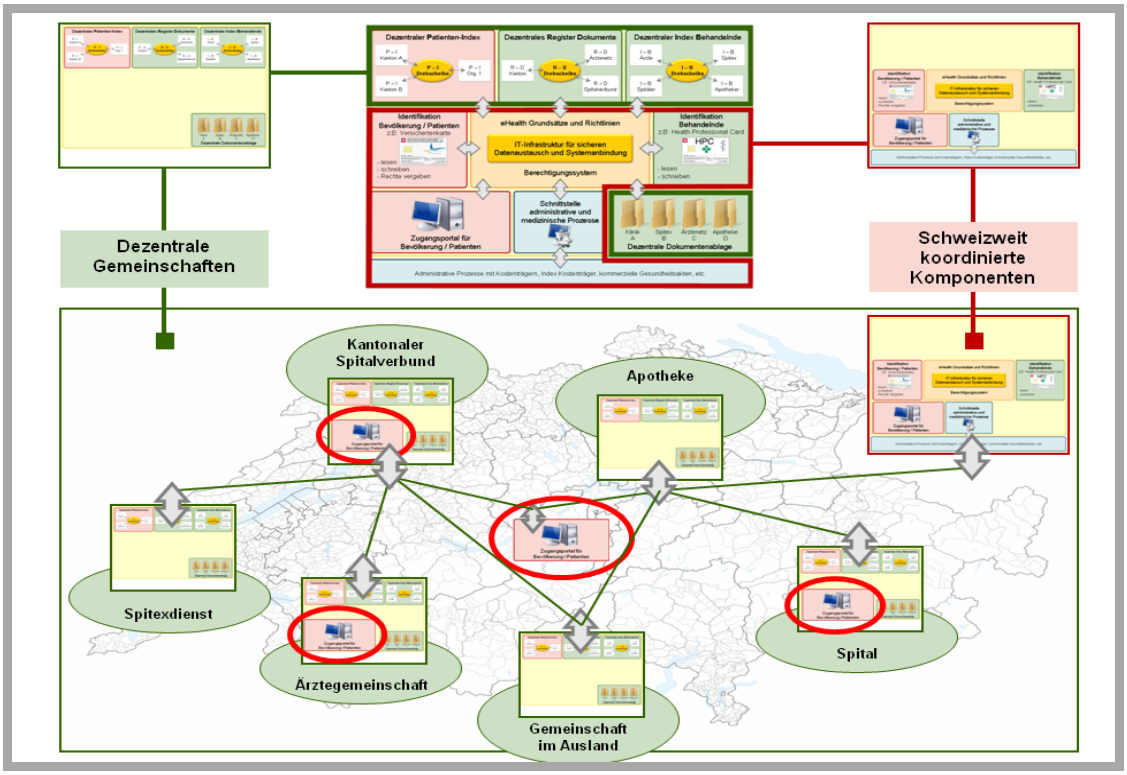


Abbildung 5: Zwei Varianten von Zugangsportalen, intern und extern

Bei der Kommunikation zwischen den Gemeinschaften besteht die Einschränkung, dass gegenseitig nur ein Lesezugriff besteht. Behandelnde, die Mitglied einer Gemeinschaft sind, können somit nur in ihrer Gemeinschaft Dokumente für Patienten einstellen. Patienten können nur über das interne Zugangsportal der von ihnen gewählten Stammgemeinschaft selber Dokumente in ihr eigenes Patientendossier einstellen. Die Verwaltung der Berechtigungen durch den Patienten erfolgt ausschliesslich in der Stammgemeinschaft (siehe Tabelle in Kapitel 1.3).	Nur Lesezugriff zwischen Gemeinschaften
Für eine schnellere Verbreitung und Akzeptanzförderung von „eHealth“ könnte es wichtig sein, den Behandelnden, welche nicht oder noch nicht Mitglied einer Gemeinschaft sind, einen einfachen und sicheren Zugang zum EPD zu ermöglichen. Damit besteht grundsätzlich eine technische Möglichkeit des lesenden Zugriffs für den Behandelnden als weiterer Benutzer eines externen Zugangsportals, solange der Patient diesen explizit gewährt hat. Durch diese Option des „einfachen“ Zugangs zum EPD-System könnte die Motivation der Behandelnden abnehmen, Mitglied einer Gemeinschaft zu werden. Die Fragestellung, ob den Behandelnden dieser nur lesende Zugang und gegebenenfalls für wie lange ermöglicht wird, ist im Rahmen der Gesetzgebungsprojekte zu klären.	externes Zugangsportal als niederschwelliger Zugang
Externe Zugangsportale ermöglichen Patienten einen lesenden Zugriff auf ihre Daten im elektronischen Patientendossier. Behandelnde, die nicht Mitglied einer Gemeinschaft sind, haben über externe Zugangsportale lesenden Zugriff auf das elektronische Patientendossier. Die Zugriffsberechtigung muss explizit durch den Patienten erteilt werden.	Empfehlung 19 externes Zugangsportal für Patienten und Behandelnde
Patientinnen und Patienten sollen selbständig Daten, wie beispielsweise Verfügungen oder Verlaufsdaten zu Körpergewicht oder Blutdruck über das interne Zugangsportal zugänglich machen können.	Dokumente von Patienten
Das Einstellen von Dokumenten ist über interne Zugangsportale *innerhalb* von Gemeinschaften möglich. Zusätzlich können andere Dienste (z.B. Webservices) innerhalb der Gemeinschaft genutzt werden. *Unabhängige* externe Zugangsportale, die nicht Bestandteil einer Gemeinschaft sind, erlauben nur den gemeinschaftsübergreifenden lesenden Zugriff.	Empfehlung 20 Einstellen von Dokumenten
Interne Zugangsportale von Gemeinschaften, die das Hochladen von Dokumenten unterstützen, sind verpflichtet, die Identität und die Rolle (Patient oder Behandelnder) des hochladenden Anwenders in den Metadaten zum Dokument zu speichern. Aus Gründen der Beurteilbarkeit der Datenvalidität muss in der Dokumentendarstellung grafisch ein klarer Unterschied zwischen Uploads eines Behandelnden oder eines Patienten gemacht werden (zum Beispiel durch optisch getrennte Bereiche).	Pflicht zur Kontrolle der Identität
Das Zugangsportal (intern oder extern) stellt geeignete Viewer zur Anzeige der in den Metadaten definierten Dokumententypen bereit. In der Benutzeroberfläche muss klar ersichtlich sein, ob die Daten vom Patienten oder von Behandelnden eingestellt wurden.	Empfehlung 21 Anzeigen von Daten
Der Verwaltung digitaler Identitäten kommt im gemeinschaftsübergreifenden Datenaustausch eine besondere Bedeutung zu. Zugangsportale (intern oder extern) übernehmen diese Verantwortlichkeiten und vergeben die Identitäten selbständig oder beziehen sie von einem Identity Service. Solange die Frage nach dem nationalen Patienten-/Personen-Identifikator	Rolle des Portals bei der Identifikation

nicht beantwortet ist, vergibt das Zugangsportal die Identifikationen nach eigenen Richtlinien. Voraussetzung dabei ist, dass die Identifikationen innerhalb der herausgebenden Stelle eindeutig sind. Dafür kann das OID-Konzept herangezogen werden, welches garantiert, dass mit Root-ID und Child-ID alle Identifikatoren eineindeutig sind.

Registrierung

Jede Gemeinschaft und jedes externe Zugangsportal muss bei der Registrierung von Anwendern sicherstellen, dass deren Identität auch die korrekten Metadaten zugeteilt werden (zum Beispiel Name, Vorname, Geschlecht, Geburtsdatum und verschiedene Identifikationen aus anderen Gemeinschaften). Diese Attribute werden bei gemeinschaftsübergreifenden Abfragen mitgegeben - zum Beispiel HPI-Serviceabfrage, Dokumentenabfragen, Berechtigungsabfrage an Stammgemeinschaft.

Die von den Zugangsportalen unterstützten Authentisierungsmittel für die Anwender müssen intern registriert und gepflegt werden. Diese müssen alle relevanten Metadaten der Personenidentifikation enthalten für das Login.

Jeder dieser gültigen Anwender, die sich als Patient oder Behandelnder registriert haben, können sich damit am Zugangsportal anmelden. Es können mehrere Authentisierungsmittel verwendet werden, die im zukünftigen Recht zugelassen werden - zum Beispiel Smartcard, USB-Stick mit Signatur, SMS-TAN-Verfahren, etc.

Der Portalanbieter wählt, welche der rechtlich zugelassenen Authentisierungsmittel bei seinem Portal von den Anwendern unterstützt werden.	Empfehlung 22 Wahl der Mittel zur Authentisierung

Transparenz und Vertrauen

Bei den Hauptanwendungsfällen für die Zugangsportale geht es um die administrativen und medizinischen Daten eines Patienten. Andere „fremde“ Informationen können aber grundsätzlich auch in den Portalen integriert werden, solange diese Informationen klar getrennt vom elektronischen Patientendossier sind - zum Beispiel externe Informationen zu Krankheiten oder Therapien, Links zu Gesundheitsforen oder deklarierte Werbeinformationen.

Um die Transparenz und Vertrauenswürdigkeit zu stärken, wird angeregt:

- auf dem Portal eine Suchmaschine anzubieten, die nur transparente und vertrauenswürdige Informationen vermittelt, z.B. HONcode-zertifizierte Websites;
- nur Links zu vertrauenswürdigen Gesundheitswebsites anzugeben, d.h. Seiten, die den HONcode-Verhaltenskodex berücksichtigen oder die HONcode-zertifiziert sind;
- Verzeichnisse von Gesundheitspartnern und -dienstleistern zur Verfügung zu stellen (Notfalldienste, Spitäler, Kliniken, Ärzte, Versicherungen);
- den Endbenutzer klar zu informieren über die Informationsquellen, so dass die Glaubwürdigkeit des Portals gestärkt wird;
- alle Zielgruppen darüber anzuleiten, wie das Portal zu verwenden ist.

Ergänzende Zertifizierungen durch weitere Qualitätslabels sind möglich.

Zugangsportale erfüllen den HONcode der Health on the Net Foundation: Die Standards, Prinzipien und Guidelines zur Qualität von Gesundheitsinformationen, der Zugänglichkeit und Benutzerfreundlichkeit des Zugangsportals werden in allen Prozessen berücksichtigt.	Empfehlung 23 HONcode Zertifizierung

Zugangsportale sind von allen Patienten unabhängig von deren körperlichen oder technischen Möglichkeiten uneingeschränkt benutzbar. Um den barrierefreien Zugang zum Portal zu optimieren, wie es für die HONcode-Zertifizierung erforderlich ist, wird empfohlen, die Richtlinien des World Wide Web Consortium (W3C) für barrierefreie Webinhalte (WCAG) 2.0 sowie die User Agent (Web-Browser, Mediaplayer) Guidelines zu befolgen. Barrierefreiheit kann von Portalanbietern als Differenzierungsmerkmal genutzt werden.	Empfehlung 24 Barrierefreiheit

6 Schlussbemerkungen

Fazit

Die Empfehlungen IV liefern fehlende Definitionen und Spezifikationen der übergeordneten zentral zu regelnden Komponenten und Dienste. Damit soll es möglich sein konkrete Umsetzungen des Reifegrades 2 im dokumentenzentrierten Umfeld zu starten und die wichtigen Themen wie Zugriffssteuerung und Audit/Protokollierung über Gemeinschaftsgrenzen hinweg anzugehen. Ohne die nähere Beschreibung der schweizweiten Komponenten ist der Datenaustausch zwischen Gemeinschaften nicht möglich.

Nächste Schritte

Für die nächste Phase ab 2013 ist vorgesehen, die Arbeiten im Bereich "Standards und Architektur" auf drei Schienen voranzutreiben. Einerseits muss für den Start in strategiekonformen Umsetzungsprojekten vertieft aufgezeigt werden, wie die bisherigen Empfehlungen I bis IV umgesetzt werden können. Andererseits sind die bisherigen Erkenntnisse so zu verbreitern und zu ergänzen, dass die Umsetzungsprojekte optimal unterstützt werden können. Darüber hinaus muss angedacht werden, wie das bisherige Konzept weiterentwickelt werden kann, damit es auch zukünftigen Anforderungen gerecht wird. Die Priorisierung der unten aufgeführten Themen wird im Rahmen der Zeitplanung festgelegt.

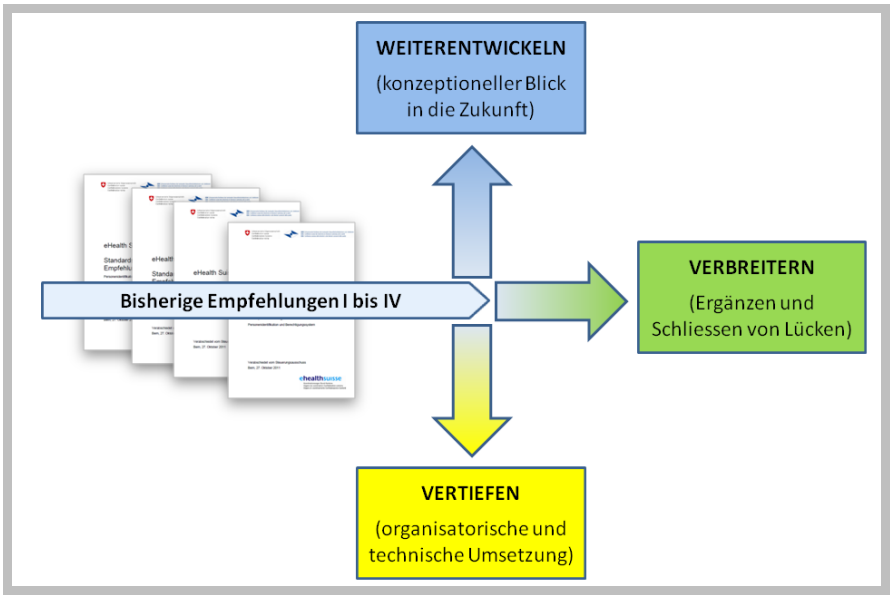
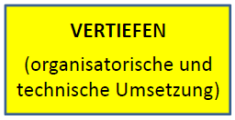


Abbildung 6: Planungsdimensionen für weitere Arbeiten

Schiene 1: Vertiefen

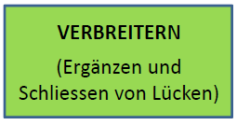
Detaillierte Beschreibung der organisatorischen und technischen Umsetzung der bisherigen Empfehlungen:

- Leitfaden für den Aufbau von Gemeinschaften (konzeptuelle Beschreibung des Zusammenspiels der Empfehlungen I bis IV);
- Technische Anleitung für die Umsetzung der Empfehlungen I bis IV (Leitfaden für die technische Implementierung).



Ergänzen von notwendigen Elementen und Füllen von Lücken in der bisherigen Konzeptarbeit:

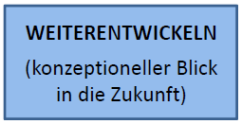
Schiene 2: Verbreitern



- Festlegung des Vorgehens für die Erarbeitung von Inhalten des elektronischen Patientendossiers, insbesondere Koordination der Experten;
- Behandlungskontext und Berechtigungen: Für eine praxisnahe Steuerung von Zugriffsrechten unter Nutzung von Identifikationsmerkmalen und Dokumenten-Metadaten muss der Behandlungskontext korrekt erfasst werden (auswählen der Wertebereiche der Metadaten und Attributsliste der zentralen Services sowie Festlegen der XCA-Metadaten für eine "Startkonfiguration");
- Prüfen einer technischen und organisatorischen Zwischenlösung für die zentralen Services, insbesondere der HPI- und HOI-Services;
- Definition der Architekturkomponente "Schnittstelle administrative und medizinische Prozesse (insbesondere die Funktionalität Export/Import für EPD-Dokumente, Rechteattribute, Einwilligungserklärungen).

Konzeptionelle Weiterentwicklung der bisherigen Grundlagen von "Standards und Architektur:

Schiene 3: Weiterentwickeln



- Ausblick in Richtung Reifegrad 3 (siehe Seiten 4 und 5), insbesondere der Umgang mit strukturierten medizinischen Informationen, die über die Grenzen von Gemeinschaften hinweg von mehreren Behandelnden gepflegt werden ("shared documents");
- Konzept für das Löschen von Daten: Was passiert wenn ein Patient ablebt oder er die Gemeinschaft verlässt ? Festzulegen ist eine einheitliche Regelung unter Wahrung der Datenschutzrichtlinien sowie deren technische Umsetzung.

Weitere wichtige Themen wie Zertifizierungsvoraussetzungen und Definition der nicht-funktionalen Anforderungen für Gemeinschaften und Zugangsportale werden im Rahmen des elektronischen Patientendossiergesetz-Projektes weiter verfolgt.

Verantwortlichkeiten im Kontext des EPD-Gesetzesprojekts

Der Steuerungsausschuss von „eHealth Suisse“ empfiehlt allen Akteuren im Sinne des Investitionsschutzes bei zukünftigen Neu- und Ersatzinvestitionen im IT-Bereich die Einhaltung der vom Teilprojekt „Standards und Architektur" empfohlenen technischen Lösungen und Ansätze im eigenen Verantwortungsbereich sicherzustellen.

Einhaltung der Empfehlungen als Investitionsschutz

Anhang 1: Relevante Architekturgrundlagen

Die nachfolgend genannten Empfehlungen I-III des Teilprojektes Standards und Architektur sind zu finden unter: http://www.e-health-suisse.ch/umsetzung/00146/00148/index.html?lang=de

1. Die Standardisierung erfolgt prozessorientiert mit Anwendungsfällen basierend auf der IHE Initiative (Integrating the Healthcare Enterprise, www.ihe.net), insbesondere mit den Integrationsprofilen der Domäne IT-Infrastructure
   [Empfehlungen I], S. 7
2. Basiskomponenten der Architektur „eHealth Schweiz“
   [Empfehlungen I], S. 6
3. Der Dokumentenaustausch in der Schweiz basiert auf gleichberechtigten Gemeinschaften, die über einen oder mehrere Zugangspunkte kommunizieren.
   [Empfehlungen II], Empfehlung 1, S. 10
4. Es wird ein Schweiz weites Verzeichnis der Gemeinschaften geführt. Nur diese erhalten die Möglichkeit, am Dokumentenaustausch teilzunehmen.
   [Empfehlungen II], Empfehlung 3, S. 12
5. In einem schweizweiten Verzeichnis werden alle zugelassenen Rollen geführt. Jede Rolle wird durch eine Rollen-Identifikation eindeutig gekennzeichnet.
   [Empfehlungen II], Empfehlung 5, S. 15
6. Die Einwilligung des Patienten, dass eine bestimmte Person in Wahrnehmung einer bestimmten Rolle für eine bestimmte Zeitdauer Zugriff auf bestimmte Dokumente hat, soll in Form eines sogenannten „Patient Consent“ festgehalten werden.
   [Empfehlungen II], Empfehlung 6, S. 17
7. Einschlusslisten (sogenannte „whitelists") enthalten Identitäten von Personen, die auf Dokumente eines Patienten zugreifen dürfen, z.B. Person des Vertrauens. Ausschlusslisten (sogenannte „blacklists“) enthalten Identitäten von Personen, denen der Zugang zu Dokumenten des Patienten verwehrt ist. Dafür muss den Personen eine Identität zugeordnet werden können.
   [Empfehlungen II], Empfehlung 7, S. 17
8. Startkonfiguration Metadaten
   [Empfehlungen II], Empfehlung 9, S. 21
9. Um eine eindeutige Identifikation von Personen zwischen Gemeinschaften zu erreichen, soll eine Schweiz weit eindeutige Kennzahl verwendet werden. Sie kann zusammen mit anderen Merkmalen für die Personenidentifikation zwischen Gemeinschaften verwendet werden. Dies gilt für Behandelnde und Patienten.
   [Empfehlungen III], Empfehlung 1, S. 14
10. Es ist eine starke Authentisierung durch eine geeignete Kombination von Wissen, Besitz und biometrischen Merkmalen anzuwenden.
    [Empfehlungen III], Empfehlung 2, S. 15
11. Einwilligung und Zugriffsrechte
    [Empfehlungen III], Empfehlung 3, S. 17
12. Definition der Vertraulichkeitsstufen
    [Empfehlungen III], Empfehlung 4, S. 17
13. Rechte bei der grundsätzlichen Einwilligung
    [Empfehlungen III], Empfehlung 5, S. 20
14. Rechte unter Verwendung der Rollen
    [Empfehlungen III], Empfehlung 6, S. 21
15. Individuelle Festlegung der Zugriffsrechte
    [Empfehlungen III], Empfehlung 7, S. 21

16. Alle Einwilligungen und Vergabe von Rechten eines Patienten werden in einer Gemeinschaft verwaltet. Diese Gemeinschaft wird als Stammgemeinschaft bezeichnet. Sie muss zwingend eine zertifizierte Gemeinschaft sein. Der Patient hat die freie Wahl, eine der zertifizierten Gemeinschaften als seine Stammgemeinschaft auszuwählen. Es gibt kein zentrales Register, in dem die Zugehörigkeit der Patienten zu ihrer Stammgemeinschaft geführt wird.
    [Empfehlungen III], Empfehlung 8, S. 22
17. Nachverfolgbarkeit, Historisierung und Audit
    [Empfehlungen III], Empfehlung 9, S. 22

Anhang 2: Technische Umsetzungshinweise

Technische Hinweise "zentrale Dienste"

Versionierung Verzeichnisdienst der Gemeinschaften und externe Zugangsportale

Für eine vertrauenswürdige Kommunikation zwischen den Gemeinschaften ist es notwendig, dass auch die zentralen Services den hohen Qualitätsansprüchen genügen. Dafür sind diese ebenfalls technisch zu prüfen. Eine eindeutige Versionierung aller Services und Verzeichnisse ist notwendig für alle Anfragen und Antworten im System. Der Verzeichnisservice der Gemeinschaften und externen Zugangsportale (CPI-S) beinhaltet eine Versionierung mit allen Versionsständen.

Verzeichnisdienst der Gemeinschaften und externe Zugangsportale notifiziert

Die Gemeinschaften müssen informiert werden, wenn es Änderungen in der Liste der zertifizierten Gemeinschaften gibt. Nur dann können sie bei einer Abfrage alle möglichen Quellen von Informationen eines Patienten erschliessen. Alle Gemeinschaften werden aktiv vom Verzeichnisservice der Gemeinschaften und externe Zugangsportale über Änderungen informiert. Dies wird als Auslöser für eine Aktualisierung der Liste der zertifizierten Gemeinschaften und externe Zugangsportale benutzt.

Technische Hinweise "Identifikation und Authentisierung"

Identifikation aller Systemteilnehmer gemäss OID-Konzept

Damit Einverständniserklärungen und Berechtigungen korrekt angewendet werden können, ist eine weltweit eindeutige Identifizierung der Systemteilnehmer notwendig. Weil es immer unterschiedliche organisatorische Stellen geben wird, welche Systemteilnehmer identifizieren, führt nur eine Kombination der Personenidentifikation und der Identifikation der herausgebenden Stelle zu einer weltweiten Eindeutigkeit (z.B. GS1 GLN eines Arztes und OID für GS1 GLN; 7601234567890 und 1.3.88 oder 2.51.1.3). Das OID-Konzept für die Schweiz wurde 2010 vom Steuerungsausschuss von „eHealth Suisse“ verabschiedet.

Pointer auf X-Assertion Provider in CPI-S

Für eine nachhaltige Implementierung des Integrationsprofils IHE:XUA über gemeinschaftsgrenzen hinweg sollte eine weitere Information in dem Verzeichnisservice der Gemeinschaften (CPI-S) vorgesehen werden. Die Responding Gateways können so herausfinden, wie die Assertion Provider in den Initiating Gateways zu finden sind. Das Verzeichnis der Gemeinschaften verwaltet sogenannte Pointer (Verweise) auf X-Assertion Provider und stellt sie und Webservice den Responding Gateways zur Verfügung.

Technische Hinweise „Berechtigungskonzept“

Basierend auf den Empfehlungen II und III ist ein Zusammenspiel verschiedener Systemkomponenten und Informationsobjekte notwendig damit die Berechtigungssteuerung allen Anforderungen gerecht wird. Wie im obigen Kapitel 3.2 beschrieben wird ein verteiltes Management von Personen und Zugriffen vorgesehen. Nachfolgend wird die Sequenz bei einer Datenabfrage über Gemeinschaftsgrenzen hinweg beschrieben:

1. In der anfragenden Gemeinschaft wird die Identität des anfragenden Behandelnden überprüft;
2. Die SAML Assertion enthält einen Behandelnden Identifikator (z.B. GS1 GLN);
3. Suche in Stammgemeinschaft und Holen der Rechteattribute;
4. Ergänzen der SAML Assertion um die Rechteattribute (inkl. Patienten ID);
5. Im Initiating Gateway prüfen, ob die Anfrage zulässig ist (Repository anfragen);
6. Ergänzen aller Patientenidentifikatoren der anderen Gemeinschaften;
7. Senden der Anfrage an alle responding Gateways für die ein Patientenidentifikator existiert;
8. Responding Gateway leitet die Anfrage in die eigene Gemeinschaft weiter;
9. Die Gemeinschaft verarbeitet die Anfrage und prüft die Berechtigung aller Resultate. Im Normalfall ist die Rechteprüfung integraler Bestandteil von Registry und Repository;
10. Die Antwort kommt zum Responding Gateway und wird weitergleitet an den Initiating Gateway sofern die Berechtigung vorhanden war;
11. Der Initiating Gateway prüft für die eigenen Gemeinschaft die Antwort (Registry Anfragen);
12. Der Initiating Gateway wartet bis alle Antworten zurück sind oder bis eine Zeitüberschreitung signalisiert wird;
13. Der Initiating Gateway kombiniert die Antworten und liefert diese zurück an die anfragende Stelle;

Da die antwortende Gemeinschaft nicht immer die Stammgemeinschaft sein wird, ist ein Übertragungsmechanismus notwendig zwischen Gemeinschaften für die Rechteattribute eines Patienten. Daraus folgt: Wenn die Stammgemeinschaft im System „eHealth“ Schweiz nicht verfügbar ist und somit nicht auf Rechteattribute des Patienten zugegriffen werden kann, werden leere Resultatlisten zurückgegeben.

Rechteattribute als Teil der SAML Assertion

Rechteattribute werden vor deren Übermittlung durch die entsprechende Stelle der Stammgemeinschaft des Patienten als XML File (Rechteattribute-Set) aufbereitet und digital signiert. Für die Übermittlung zwischen den Gemeinschaften wird dieses Rechteattribute-Set als Attribut in die SAML Assertion integriert.

Rechteprüfung durch Responding Gateway

Der Responding Gateway prüft den Inhalt der gelieferten Identifikation und Attributen (via SAML Assertion aus IHE:XUA) mit den aktuell geltenden Berechtigungen und kann damit über Zugriff oder Verweigerung entscheiden. Der Responding Gateway wird damit zum Access Enforcement Point, der zwischen Gemeinschaften entscheidet, ob eine Transaktion erlaubt ist oder nicht.

Der Zusammenhang zwischen dem verteilten Identity und Access Management (IAM) und dem Access Enforcement Point ist in Abbildung 7 schematisch dargestellt.

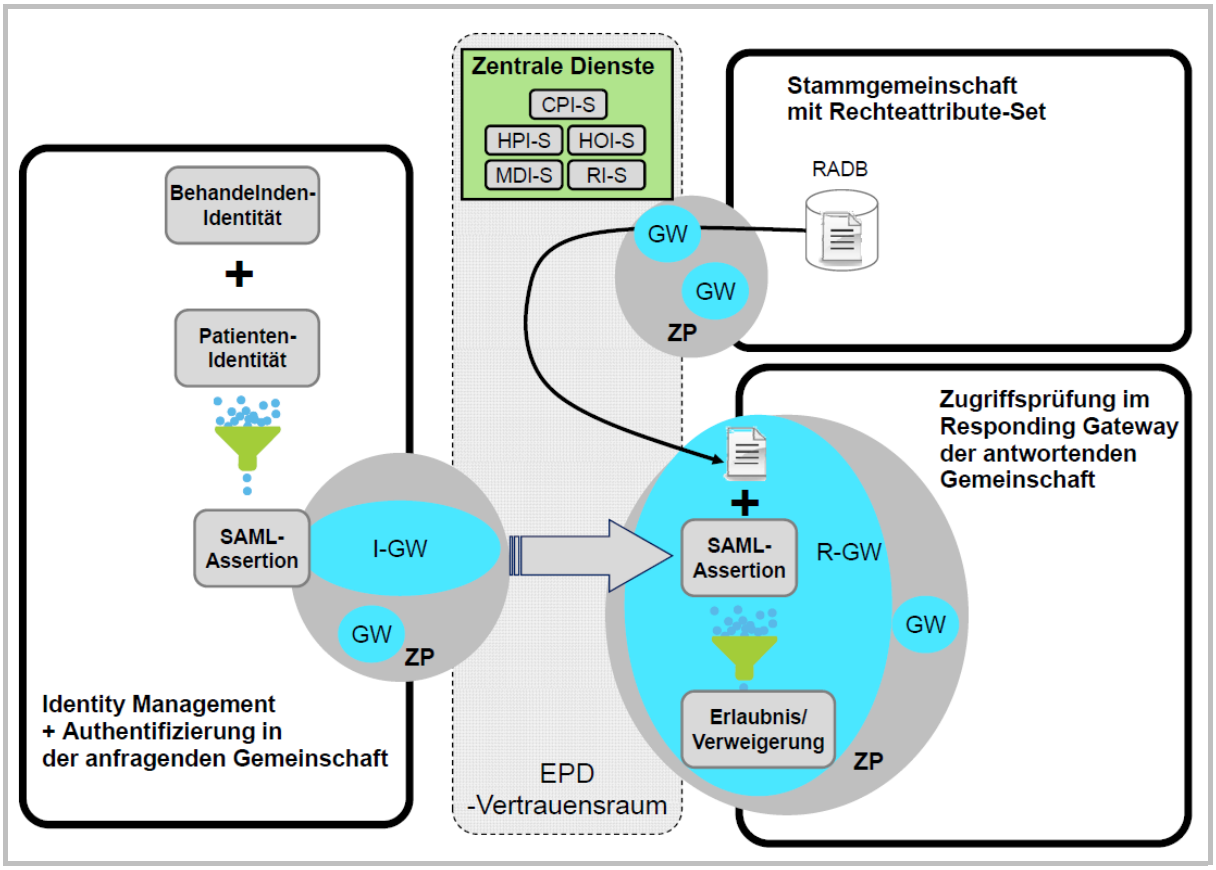


Abbildung 7: Zusammenspiel im Berechtigungskonzept

Technische Hinweise „Audit und Notifikation“

Das IHE Profil ATNA (Audit Trail and Node Authentication) definiert wie Hosts geschützt werden, sowie wie und welche Informationen sie protokollieren. Die im Rahmen von ATNA erstellten Audit Logs weisen eine feine Granularität auf und sind sehr technisch. ATNA beschränkt sich auf eine „IHE affinity domain" und definiert keine gemeinschaftsübergreifenden Zugriffe.

Umsetzung mit IHE Profilen

Weil alle teilnehmenden Systeme und Anwendungen zeitliche Abhängigkeiten haben und ihre Ereignisse mit verlässlichen Zeitstempeln loggen müssen, müssen ihre Zeiten synchronisiert werden.

Gemeinschaften synchronisieren ihre Systeme gemäss IHE Integrationsprofil Consistent Time (CT).

Zeitsynchronisation gemäss IHE:CT

Gemeinschaften protokollieren die Trigger-Ereignisse gemäss IHE Integrationsprofil Audit Trail and Node Authentication (ATNA) in einem lokalen

Trigger-Ereignisse gemäss IHE:ATNA

Systemlog.

Anhang 3: Attribute CPI-S (Verzeichnisdienst der Gemeinschaften und externen Zugangsportale)

Attribut	Name lang	Erläuterung
ComName	Gemeinschaftsname	Name der Gemeinschaft. Diese Bezeichnung muss eindeutig und selbsterklärend sein. Sie wird dazu verwendet um die Gemeinschaft im Portal zu benennen und kann von Patienten oder Behandelnden bei der Wahl der Stammgemeinschaft oder beim Definieren von Rechteattributen genutzt werden.
ComInfo	Information zur Gemeinschaft	allgemeine beschreibende Informationen zur Gemeinschaft (Freitext, max. 500 Zeichen)
ComLogo	Logo der Gemeinschaft	bildliches Logo der Gemeinschaft im JPG Format
ComLegal	rechtliche Grundlagen für die Gemeinschaft	beschreibender Freitext über die rechtlichen Grundlagen der Gemeinschaft, z.B. mit Verweis auf kantonales Gesundheitsgesetz oder nationales Elektronisches Patientendossiergesetz oder private Vereinbarungen auf Gemeinschaftsebene
ComContact	Kontaktinformationen der Gemeinschaft	Um mit der Gemeinschaft in direkten Kontakt zu treten werden die Kontaktinformationen im CPI-S hinterlegt. Diese Information wird von anderen Gemeinschaften an Behandelnde und Patienten weitergegeben. Für die Zusammenarbeit zwischen den Gemeinschaften ist ein zweiter (technischer) Kontakt zu hinterlegen, der aber nur für interne Zwecke verwendet werden darf. Zu jedem Kontakt sind mindestens zwei mögliche Kontaktmethoden zu hinterlegen. (Postadresse, E-Mail und Telefon).
ComOID	OID der Gemeinschaft	Jede Gemeinschaft muss eine eindeutige OID erhalten, welche die Gemeinschaft weltweit eindeutig identifiziert. Diese muss im Schweizer OID-Register gelistet sein.
ComAuthN	Authentisierungsprovider der Gemeinschaft	Jede Gemeinschaft muss mindestens einen Authentisierungsprovider haben, der die SAML Assertions im Namen der Gemeinschaft unterschreibt. In diesem Attribute werden alle aktuell gültigen X.509 Zertifikate hinterlegt.
ComAssert	Assertion Authority der Gemeinschaft	jede Gemeinschaft muss für die Rolle als Stammgemeinschaft einen Assertion Service betreiben, welche dir digitalen Signaturen der Rechteattribute vornehmen kann. Die zur Prüfung solcher Signaturen nötigen Informationen werden im CPI-S hinterlegt.
ComXPoint	Pointer auf X-Assertion Provider	Abrufbare Information für Responding Gateways die die Assertion Provider in den Initiating Gateways kontaktieren wollen

Attribut	Name lang	Erläuterung
ComGW	Zugangspunkt der Gemeinschaft	Jede Gemeinschaft muss mindestens einen Gateway betreiben, welcher die Kommunikation zwischen den Gemeinschaften abwickelt. In diesem Attribut werden die URLs der Gateways hinterlegt.
ComVersion	Version der Gemeinschaft	für welche Version der Gateways ist die Gemeinschaft zertifiziert
ComZert	Datum der Zertifizierung	das Datum der erfolgreichen Zertifizierung bzw. Rezertifizierung